UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,155	11/03/2003	Massimiliano Antonio Poletto	12221-025001	5551

26161 7590 03/19/2008
FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
BARQADLE, YASIN M	
ART UNIT	PAPER NUMBER
2153	
MAIL DATE	DELIVERY MODE
03/19/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/701,155	POLETTO ET AL.	
	Examiner	Art Unit	
	YASIN M. BARQADLE	2153	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 December 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/21/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Amendment

Applicant's arguments filed on December 21, 2007 have been considered but are not deemed persuasive.

Response to Arguments

Applicant's arguments regarding the 101 rejection is not persuasive. A memory for storing a data structure for tracking network behavior, comprising: a connection table containing a record object that stores information about traffic to or from the node and between that node and others nodes in the network fits a data structure with mere arrangements of data in a table. Therefore it is a non-statutory subject matter.

Applicant's arguments regarding the double patenting rejection are not persuasive.

Claims 1 and 14 of Copending Application **10/701154 and** Claims 1, 19 and 25 of Copending Application **10/701356** contain every element of claim 1 of the instant application and as such anticipate(s) claim 1 of the instant application. Therefore, the narrower claims of the co-pending invention anticipate the broader claims of the instant application. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed.

"A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or **anticipated by**, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus). " ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

The Applicant argues that Tams "does not provide any mechanism to map each node of a network to a record object that stores information ... to or from the node and between that node and other nodes in the network." (Page 9, second paragraph).

Examiner respectfully disagrees. Tams' Table 2 and ¶ 0210 show a connection table that maps each node (identified by an IP address 123.45.67.89) to a record object (host object/or destination IP address 98.76.54.32) and traffic information such as protocols used (IP/TCP/FTP) and number of packets in the conversation between the hosts. Furthermore Tams teaches "Two conversations were detected during this first hourly time period. A first conversation between devices A and B which involved 10 packets and a second conversation between

devices A and E which involved 6 packets. The number of bytes, in addition to the number of packets, may also be stored in each record of the database 707." (Para. 210).

Applicant also argues that Tams "does not show a table indexed by source address or by destination address or by time (page 10 paragraph 5), but merely that the table has source and destination addresses stored therein for a particular entry." (Page 10 third paragraph).

The Examiner respectfully disagrees. The Applicant did not explain how a table listing traffic information between nodes by source and destination address as shown by Tam's table 2 is different the Applicant's claimed connection table. Examiner believes Tams' table 2 meets the Applicant's argued limitation. As to indexing by time. Tams clearly show time stamp traffic information indicating the conversation between hosts that is stored in a database by different time interval. See ¶0198 and ¶0201-0208 and the time scale data structure 709,711,713 and 715 in fig. 7.

The Applicant also argues "Maufer does not teach "the addresses indexing the connection include a physical layer address to IP address map that is used to determine Host ID." Page 12. The Examiner notes that Maufer discloses a

physical [layer] address to IP address map that is used to determine Host ID (col. 16, line 51-65 and table 300, fig. 5A. See also col. 5, lines 36-60).

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 1 is rejected under 35 U.S.C. 101 because it is directed to a data structure ("A memory for storing a data structure for tracking network behavior, comprising: a connection table ...". When nonfunctional descriptive material is recorded on some memory, it is not statutory since no requisite functionality is present to satisfy the practical application requirement. Merely claiming nonfunctional descriptive material, i.e., abstract ideas, stored in a memory, does not make it statutory.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to

prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-17 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-22 of copending Application No. 10701154 and claims 1-36 of copending Application No. 10701356. Although the conflicting claims are not identical, they are not patentably distinct from each other a comparison between instant application independent claim 1 and the claims 1 and 14 (of the copending application number 10701154) and claims 1, 19, and 25 (of the copending application number 10701356) reveal the copending claims are simply species of the broader claim 1 of the instant application. Hence, claim 1 of the instant application is generic to the species of the invention covered by independent claims of the copending applications stated above. Thus, the broad generic invention is anticipated by the narrower species of the co-pending invention, thus without a terminal disclaimer, the species claims preclude issuance of the generic application. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993).

Instant Application **10/701155**	Copending Application **10/701154**	Copending Application **10/701356**
Claim 1: A memory device storing a data structure for tracking network behavior, comprising:	Claims 1: A system, comprising: a plurality of collector devices that are disposed to collect statistical information on packets that are sent between nodes on a network;	Claims 1: A device comprising: ---------- a processor; ---------- ----------

a connection table that maps each node of a network to a record **object that stores information about traffic to or from the node** and between that node and others nodes in the network. 1	--- ---**an aggregator that receives network data from the plurality of collector devices,** and **which produces a connection table that maps each node on the network to a record that stores information about traffic to or from the node.** Claim 14, A method, comprises: providing a plurality of collector devices in a network to collect statistical information on packets that are sent between nodes on a network; and sending statistical information from the collector devices to an aggregator, the aggregator --- **producing a connection table that maps each node on the network to a record that stores information about traffic to or from the node** 1 and 14	a memory storing **a connection table that maps each node of a network to** a host **object, the connection table stores information about traffic to or from the node.** Claim 19, A computer program product residing on a computer readable medium for use in detecting network intrusions comprises instructions for causing a processor to: --- store a **connection table that maps each node of a network** to a host **object, the connection table stores information about traffic to or from the node** 1, 19 and 25
2	8 and 17	5
3	9 and 18	6

4	10 and 19	7
5	11 and 20	8
6	12 and 21	9 and 30
7 and 8	13 and 22	10 and 31

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1–9 and 11, 13-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Tams et al U.S. Publication Number (20030069952), hereinafter "Tams".

As per claim 1, Tams (20030069952) teaches a memory device (fig. 2, 162) storing a data structure for tracking network behavior (¶ 0079-0081 and ¶0198), comprising:

a connection table (fig, 2, data table and Table 2, page 11) that maps each node of a network to a record object that stores information about traffic to or from the node and between that node and others nodes in the network (¶ 0157-0164 and ¶0210. See TABLE 2, page 11).

As per claims 2 and 3, Tams teaches wherein the connection table includes a plurality of records that are indexed by source and destination address (See TABLE 2, page 11).

As per claim 4, Tams teaches the device of claim 1 wherein the connection table includes a plurality of records that are indexed by time (¶0198 and ¶0201-0206; see steps in fig. 8).

As per claim 5, Tams teaches the device of claim 1 wherein the connection table includes a plurality of records that are indexed by source address, destination address and time (See TABLE 2, page 11 and ¶ 0198 and ¶ 0201-0206).

As per claim 6, Tams teaches the device of claim 1 wherein the connection table is a plurality of connection sub-tables each sub-table having data pertaining to network traffic over different time scales (¶0198 and ¶0201-0208; see the time scale data structure (709,711,713 and 715 in fig. 7).

As per claim7, Tams teaches the device of claim 1 wherein the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table. (¶0198 and ¶0201-0208; see the time scale data structure (709,711,713 and 715 in fig. 7).

As per claim 8, Tams teaches the device of claim 7 wherein the at one sub-table holds records received from all collectors over the time scale of the table (¶0198 and ¶0212).

As per claim 9, Tams teaches the device of claim 5 wherein the addresses indexing the connection table are IP addresses (See TABLE 2, page 11).

As per claim 11, Tams teaches the device of claim 1 wherein the host record of a first host also maps to a second host which communicates with the first host to a "host pair record" that has information about all the traffic from between the first and second hosts (¶0201 and ¶0209-0210).

As per claim 13, Tams teaches the device of claim 1 wherein a record stores a measure of the number of bytes, packets, and connections that occurred between hosts during a given time-period (¶ 0157-0164 and ¶0210. See TABLE 2, page 11).

As per claim 14, Tams teaches wherein data in the record is organized by well known transport protocols and well-known application-level protocols (¶ 0151-0157 and ¶0161-168. See TABLE 2 and TABLE 4A-4B in page 11).

As per claim 15, Tams teaches the device of claim 1 wherein host records have no specific memory limit (¶0202-0206).

As per claim 16, Tams teaches the device of claim 1 wherein for application-level protocols and for every pair of hosts, the connection table stores statistics for traffic between the hosts (¶ 0151-0157 and ¶0161-168. See TABLE 2 and TABLE 4A and 4C in page 11).

As per claim 17, Tams teaches the device of claim 16 wherein the connection table stores protocol-specific records as (protocol, count) key-value pairs (¶ 0151-0157 and ¶0161-168. See TABLE 2 and TABLE 4A-4B in page 11).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tams et al U.S. Publication Number (20030069952), hereinafter " Tams" in view of Maufer et al U.S. Patent Number (7120930), hereinafter " Maufer".

As per claim 10, although Tams shows substantial features of the claimed invention including a table with plurality of records, he does not explicitly show a physical [layer] address to IP address map that is used to determine Host ID.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the system disclosed by Tams, as evidenced by Maufer U.S. Patent Number (7120930).

In analogous art, Maufer whose invention is about a Method and apparatus for enhanced security for communication over a network including a mapping table accessible by a gateway computer used to form associations between a

local address for the client and a destination address for a peer and a Security Parameters Index associated with IPSec-protected traffic from the peer (abstract), discloses a physical [layer] address to IP address map that is used to determine Host ID (col. 16, line 51-65 and table 300, fig. 5A. See also col. 5, lines 36-60).

Giving the teaching of Maufer, a person of ordinary skill in the art would have readily recognized the advantage of modifying Tams by employing the enhanced network security system of Maufer for particularly identifying traffic flowing from a remote address to the local address using physical layer (MAC) address to IP address mapping in order to verify hosts belonging to the private network from unknown intruders of the public network. In this way fake packets belonging to unknown sources are recognized and discarded.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tams et al U.S. Publication Number (20030069952), hereinafter " Tams" in view of Ontiveros et al U.S. Patent Number (20020107953), hereinafter " Ontiveros".

As per claim 12, although Tams shows substantial features of the claimed invention including a connection table that enables a consuming device to obtain summary information about one host and about the traffic between any pair of hosts (¶0118), Tams does not explicitly show a two level mapping between a first one of the hosts of any pair to a second one of the hosts of the

any pair and from the second one of the host of the any pair to the first one of the host for the any pair for a second level mapping.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the system disclosed by Tams, as evidenced by Ontiveros U.S. Pub Number (20020107953).

In analogous art, Ontiveros discloses a two level mapping between a first one of the hosts of any pair to a second one of the hosts of the any pair and from the second one of the host of the any pair to the first one of the host for the any pair for a second level mapping (¶ 036-050 and abstract)

Giving the teaching of Ontiveros, a person of ordinary skill in the art would have readily recognized the advantage of modifying Tams by employing the data traffic monitoring system of Ontiveros in order to detect any suspicious packets in any direction (both incoming and outgoing) of the network data traffic. In this way unauthorized access to a network is recognized and prevented.

Conclusion

ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply

is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

The prior made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yasin Barqadle whose telephone number is 571-272-3947. The examiner can normally be reached on 9:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenn Burgess can be reached on 571-272-3949. The fax phone numbers for the organization where this application or proceeding is assigned are 703-872-9306 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained form the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either private PAIR or public PAIR system. Status information for unpublished applications is available through private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

YB

Art Unit 2153

/Krisna Lim/

Primary Examiner, Art Unit 2153